The Dissertation Committee for Laura Michelle Hitt
Certifies that this is the approved version of the following dissertation:

GENUS 2 CURVES IN PAIRING-BASED CRYPTOGRAPHY AND THE MINIMAL EMBEDDING FIELD

Committee:

José Felipe Voloch, Supervisor

John Tate

Ferdando Rodriguez-Villegas

Jeffrey Vaaler

Alice Silverberg

GENUS 2 CURVES IN PAIRING-BASED CRYPTOGRAPHY AND THE MINIMAL EMBEDDING FIELD

by

Laura Michelle Hitt, B.S.

DISSERTATION

Presented to the Faculty of the Graduate School of

The University of Texas at Austin

in Partial Fulfillment

of the Requirements

for the Degree of

DOCTOR OF PHILOSOPHY

THE UNIVERSITY OF TEXAS AT AUSTIN

August 2007

Acknowledgments

I would like to thank my advisor Felipe Voloch for his time, insight and direction in this thesis problem, and especially his assistance through many revisions. I appreciate John Tate, Fernando Rodriguez-Villegas, Jeffrey Vaaler and Alice Silverberg for their time, availability and service on my committee. I am grateful to Tanja Lange for her gracious encouragement and timely advice in various aspects of the process involved in this work. I have been inspired by the great knowledge of, and energy toward, mathematics that has been imparted in the classes and interactions I have had with each of these mathematicians over the years. I am grateful for all that I have learned as these they modeled excellence in research and teaching.

I treasure the faithful friendship of Rohit Ghosh, as we have walked through many challenges together. I thank him for all that he has invested in both my academic and non-academic life. The memories we share and conversations exchanged have significantly shaped who we are today and will be carried into tomorrow. I also thank all my friends in the Mathematics Department at The University of Texas for making this a pleasant environment in which to work, as well as the others in the various communities I have found in Austin.

I appreciate the support and patience of my dear family and mentors, especially the delightful Diane Thompson, Dr. J. Budziszewski, John Evans, Nick Repak and the Tuesday Group. Their wisdom, counsel, prayers, love and encouragement have been invaluable to me. Above all, I humbly thank God for providing the ability and resources that have enabled the completion of this pursuit.

GENUS 2 CURVES IN PAIRING-BASED CRYPTOGRAPHY AND THE MINIMAL EMBEDDING FIELD

Publication No. _____

Laura Michelle Hitt, Ph.D.
The University of Texas at Austin, 2007

Supervisor: José Felipe Voloch

A pairing-friendly hyperelliptic curve over a finite field $\mathbb{F}_q$ is one whose group of $\mathbb{F}_q$-rational points of its Jacobian has size divisible by a large prime and whose embedding degree is small enough for computations to be feasible but large enough for the discrete logarithm problem in the embedding field to be difficult. We give a sequence of $\mathbb{F}_q$-isogeny classes for a family of Jacobians of curves of genus 2 over $\mathbb{F}_q$, for $q = 2^m$, and their corresponding small embedding degrees for the subgroup with large prime order. We give examples of the parameters for such curves with embedding degree $k < (\log q)^2$, such as $k = 8, 13, 16, 23, 26, 37, 46, 52$. For secure and efficient implementation of pairing-based cryptography on curves of genus g over $\mathbb{F}_q$, it is desirable that the ratio $\rho = \frac{g \log_2 q}{\log_2 \ell}$ be approximately 1, where ℓ is the order of the subgroup with embedding degree k. We show that for our family of curves, ρ is often near 1 and never more than 2.

We construct examples to show that the minimal embedding field can be significantly smaller than $\mathbb{F}_{q^k}$. This has the implication that attacks on the DLP can be dramatically faster than expected, so there could be "pairing-friendly" curves that may not be as secure as previously believed.

Table of Contents

List of Tables

Chapter 1

Introduction

The security of public-key cryptosystems, which were introduced by Diffie and Hellman in [DH76], is based on the computational difficulty of solving the discrete logarithm problem.

Definition 1.0.1. The *discrete logarithm problem (DLP)* is as follows: given a finite cyclic group G generated by g and an element $h \in < g >$, find an integer α such that $h = g^{\alpha}$.

Discrete logarithm (DL) cryptosystems were concentrating on the multiplicative group of a finite field, but then in 1985, Koblitz [Kob87] and Miller [Mil86] independently proposed using the group of rational points on an elliptic curve on which to base a DL cryptosystem. Elliptic curves are attractive for cryptography as there is currently no sub-exponential algorithm for solving the discrete logarithm problem on properly chosen curves.

The National Security Agency states in [Age05], "Elliptic Curve Cryptography provides greater security and more efficient performance than the first generation public key techniques (RSA and Diffie-Hellman) now in use."

Koblitz also proposed using Jacobian varieties of hyperelliptic curves over finite fields to supply the group of prime order [Kob89]. With hyperelliptic curves of small genus, it is possible to work over a smaller field while achieving comparable security as in other cryptosystems.

Definition 1.0.2. The *hyperelliptic curve discrete logarithm problem (HCDLP)* is the following: Let C be a hyperelliptic curve over a finite field $\mathbb{F}_q$. Suppose P is some point of $J_C(\mathbb{F}_q)$ with large prime order and let Q be a point in $< P >$. Find an integer α such that $Q = [\alpha]P$.

Bilinear maps on certain groups used in DL cryptosystems were first used to attack cryptographic security in 1993 with the work of Menezes, Okamoto and Vanstone [MOV93]. The MOV attack used the Weil pairing on supersingular elliptic curves to transport the discrete logarithm problem on a curve defined over $\mathbb{F}_q$ to the discrete logarithm in the multiplicative group of a finite field $\mathbb{F}_{q^k}$, for some k, where there are more efficient methods for solving the DLP. In 1994, Frey and Rück [FR94] used the Tate pairing in a similar attack, and so pairings were viewed as useful for destructive purposes in cryptography.

In 2000, positive applications of bilinear maps were proposed independently in [Jou00] and [SOK00], and since then pairings on groups have been used for many constructive purposes. A few examples include a one-round three-party key agreement [Jou00] (see also [Jou04]), identity-based encryption (IBE) [BF01], and short signatures [BLS01] (see also [BLS04]).

The exponent k has become known as the *embedding degree*. For an ℓ-order subgroup of the Jacobian of a curve defined over $\mathbb{F}_q$, k is the smallest positive integer such that $q^k - 1$ is divisible by ℓ. For pairing-based cryptosystems, it is important to find curves where the embedding degree k is small enough that the pairing is efficiently computable, but large enough that the DLP in the embedding field is difficult. The common practice is to consider k/g for assessment of cryptographic security. However, this may fail to capture the security of a pairing-based cryptosystem ([Gal01a, Section 3.11],[RS02], [Sil03]). We will construct examples that show how the embedding degree can be a far from accurate measure of the size of the minimal embedding field.

We know that $k \leq 6$ for supersingular elliptic curves, as first shown in [MOV93]. Galbraith in [Gal01b] shows that $k \leq 12$ for supersingular curves of genus two, which is attained in characteristic two. It has also been shown in [GMV04] that one can obtain $k = 12$ for ordinary curves of genus two in characteristic two. In general, one expects k to be roughly the size of the large prime-order subgroup, and for cryptographic applications such a k would be much too large for the computation of pairings to be feasible.

It is also desirable for the order of $J_C(\mathbb{F}_q)$ to be prime or near-prime, since the attack of [PH78] can reduce the DLP to prime-order subgroups. Thus for a curve of genus g and embedding degree k with respect to a subgroup of prime order ℓ, one examines the ratio $\rho = \frac{g \log_2 q}{\log_2 \ell}$. For secure and efficient implementation, the ideal situation is to have $\rho \sim 1$, though currently the best ratio achieved is $\rho \sim 5/4$ [BW05].

Following [GM05], we will say that a pairing-friendly curve C over $\mathbb{F}_q$ is one that satisfies the following two conditions: (1) $\#J_C(\mathbb{F}_q)$ should be divisible by a "sufficiently large" prime ℓ so that the DLP in the ℓ-order subgroup of $J_C(\mathbb{F}_q)$ is suitably hard, and (2) the embedding degree k should be "sufficiently small" so that the arithmetic in $\mathbb{F}_{q^k}$ can be efficiently implemented, but large enough so that the DLP in the finite field withstands index-calculus attacks. We refrain from making precise these sizes at this point. Much research has focused on understanding and constructing suitable supersingular and ordinary hyperelliptic curves. We will produce parameters for a family of non-supersingular, non-ordinary curves of genus two with small embedding degree for the large prime-order subgroup of the Jacobian defined over $\mathbb{F}_q$.

Our discussion is as follows. In Chapter 2 we present the mathematical framework underlying the results of this work. Then in Chapter 3 we give our pairing-friendly curves: a sequence of $\mathbb{F}_q$-isogeny classes for a family of Jacobians of genus 2 curves over $\mathbb{F}_q$, for $q = 2^m$, and the corresponding small embedding degrees for the large prime order subgroup. We give examples of the parameters for such curves with embedding degree $k < (\log q)^2$, such as $k = 8, 13, 16, 23, 26, 37, 46, 52$. (Whenever we use $\log x$, we mean the natural logarithm of x.) We show that for our family of curves, the ratio ρ is often near 1 and never more than 2.

In Chapter 4 we discuss why the embedding degree of a curve may not necessarily correspond to the minimal embedding field, and we construct examples to show that the difference in size of the extension degrees can be significant. For a curve of any genus defined over $\mathbb{F}_q$, where $q = p^m$, the

pairing on a group of order ℓ embeds in a field that is not necessarily an extension of $\mathbb{F}_q$, but merely of $\mathbb{F}_p$. This was noted to yield a difference in field exponents by a factor of 2 in the supersingular case when ℓ is sufficiently large in [RS02]. More specifically, if $\mathrm{ord}_\ell p$ is the smallest positive integer x such that $p^x \equiv 1 \bmod \ell$, then the minimal embedding field is $\mathbb{F}_{p^{\mathrm{ord}_\ell p}} = \mathbb{F}_{p^{kD}}$, where $D = \gcd(\mathrm{ord}_\ell p, m)$. Our examples demonstrate that there can be a difference for both supersingular and non-supersingular curves and that it can grow with m. As in [RS02] and [Sil03], we advocate the use of two separate parameters: an embedding degree to indicate the field one must work over to compute the pairing, and a security parameter such as $k' = \frac{\mathrm{ord}_\ell p}{mg}$ to reflect the minimal field containing the embedding.

Chapter 2

Mathematical Framework

2.1 Curves and Jacobians

We provide the mathematical framework for hyperelliptic curves in cryptography as it pertains to our research. For a more thorough treatment, refer to [CF05, Chapters 4,6,14]. For a prime p and positive integer m, we let $\mathbb{F}_q$ be a finite field with $q = p^m$ elements. The *characteristic* of $\mathbb{F}_q$ is p, and the *extension degree* is m. We will also write $\mathbb{F}_q^* \equiv \mathbb{F}_q - \{0\}$. For any field k, we let $\overline{k}$ be an algebraic closure of k.

Definition 2.1.1. [JMS04] Let $g > 0$ be an integer. A non-singular (imaginary quadratic) *hyperelliptic curve C of genus g over a field k* is defined by an equation of the form

$$C : y^2 + h(x)y = f(x),$$

where $h, f \in k[x]$, f is monic, $\deg(f) = 2g+1$, $\deg(h) \leq g$, and if $y^2+h(u)v = f(u)$ for $(u, v) \in \overline{k} \times \overline{k}$, then $2v + h(u) \neq 0$ or $h'(u)v - f'(u) \neq 0$. In the case when $g = 1$ we call C an *elliptic curve*.

If the characteristic is not equal to two, then we can assume without loss of generality that $h(x) = 0$.

Definition 2.1.2. [JMS04] For any subfield K of $\overline{k}$ containing the field k, the set

$$C(K) = \{(x, y) : x, y \in K, y^2 + h(x)y = f(x)\} \cup \{\infty\}$$

is called the *set of K-rational points on C*. The point ∞ is called the *point at infinity* and corresponds to the only projective point at infinity that satisfies the homogenized equation. A point P on C, written $P \in C$, is a point $P \in C(\overline{k})$.

The K-rational points of an elliptic curve form a group, but this is not the case for hyperelliptic curves of genus $g \geq 2$, so one uses the group of k-rational points of the Jacobian of C. In this paper, whenever we refer to a curve as if it is a group, we mean the group $\mathbb{F}_q$-rational points of the Jacobian of the curve.

Let us review a few concepts needed to understand the construction of the Jacobian. We let K be a perfect field and G_K denote the absolute Galois group of K.

Definition 2.1.3. [CF05, Section 14.1.2] The *group of divisors of C over K of degree 0* is given by

$$\mathrm{Div}_{\mathrm{C}}^0(K) = \{D = \sum_{P \in C} n_P P \mid n_P \in \mathbb{Z},\ n_P = 0 \text{ for almost all } P \in C, \sum_{P \in C} n_P = 0,$$

$$\text{and such that } \sigma(D) = \sum_{P \in C} n_P \sigma(P) = D \text{ for all } \sigma \in G_K\}.$$

The latter condition means that the divisor is defined over K, and the condition that $\sum_{P \in C} n_P = 0$ means the divisor has degree 0.

The function field of C over K, $K(C)$, is the field of fractions of the coordinate ring, $K[C] = K[x, y]/(y^2+h(x)y-f(x))$. For a function $f \in K(C)$, $f \neq 0$, let $\mathrm{ord}_P(f)$ count the multiplicity of f at P, where $\mathrm{ord}_P(f) > 0$ if P is a zero of f, and $\mathrm{ord}_P(f) < 0$ if f has a pole at P. We can build a degree zero divisor defined over K as $\mathrm{div}(f) = \sum_{P \in C} \mathrm{ord}_P(f)(P)$. Any divisor $D = \mathrm{div}(f)$ will be called a principal divisor.

Definition 2.1.4. The *divisor class group of C over K*, denoted by $\mathrm{Pic}^0_{\mathrm{C}}(K)$, is the quotient group of $\mathrm{Div}^0_{\mathrm{C}}(K)$ by the group of principal divisors of C over K.

Hence, two divisors D and D' belong to the same equivalence class when their difference $D - D'$ is a principal divisor. There exists an abelian variety which can be defined over K, called the *Jacobian of C*, J_C, of dimension g such that $J_C(K)$ is isomorphic to $\mathrm{Pic}^0_{\mathrm{C}}(K)$ for all K.

Definition 2.1.5. If ℓ is an integer, then $J_C(K)[\ell]$ denotes the set of all ℓ-*torsion points* of $J_C(K)$, i.e. all points P over K such that $[\ell]P = O$.

Definition 2.1.6. Let $p > 0$ be the characteristic of the field K.

(i) An abelian variety A is said to have *p-rank s* if the subgroup of points of order p of $A(\overline{K})$ has cardinality p^s, that is, $A(\overline{K})[p] \simeq (\mathbb{Z}/p\mathbb{Z})^s$. By the p-rank of a curve we mean the p-rank of its Jacobian variety.

(ii) An abelian variety of dimension g is said to be *ordinary* if it has p-rank g.

(iii) An elliptic curve is *supersingular* if it has p-rank 0, and a general abelian variety is *supersingular* if it is isogenous over $\overline{K}$ to a product of supersingular elliptic curves [Oor74]. While every supersingular abelian variety has p-rank 0, the converse is only true for abelian varieties of dimension less than 2 [CF05, Remark 4.75].

The Jacobian of C defined over $\mathbb{F}_q$ has an endomorphism called the *Frobenius endomorphism*, which sends a point (x, y) to (x^q, y^q). If the Jacobian has dimension g, then the Frobenius endomorphism satisfies an integer polynomial $P(x)$ of degree $2g$, and it is known as the *characteristic polynomial of Frobenius*. If $L(t)$ is the numerator of the zeta function of the curve, then $P(x) = x^{2g}L(1/x)$, and $P(x)$ factors over the complex numbers as $P(x) = \prod_{i=1}^{2g}(x - \alpha_i)$, where $|\alpha_i| = \sqrt{q}$. This characteristic polynomial of Frobenius determines the $\mathbb{F}_q$-isogeny class of the abelian variety [Tat66].

Let C be a smooth projective curve of genus g over $\mathbb{F}_q$. Then for any integer $r \geq 1$, we have

(i) $\#C(\mathbb{F}_{q^r}) = q^r + 1 - \sum_{i=1}^{2g} \alpha_i^r$.

(ii) $\#J_C(\mathbb{F}_q) = P(1) = \prod_{i=1}^{2g}(1 - \alpha_i)$.

(iii) $(\sqrt{q} - 1)^{2g} \leq \#J_C(\mathbb{F}_q) \leq (\sqrt{q} + 1)^{2g}$.

In particular, for $g = 2$ there exist integers a_1, a_2 such that

$$\#C(\mathbb{F}_q) = a_1 + q + 1, \text{ and } \#C(\mathbb{F}_{q^2}) = 2a_2 - a_1^2 + q^2 + 1,$$

The characteristic polynomial of Frobenius is

$$f_{J_C}(t) = t^4 + a_1 t^2 + a_2 t^2 + q a_1 t + q^2,$$

where the a_1 and a_2 determine the $\mathbb{F}_q$-isogeny class of J_C, and

$$\#J_C(\mathbb{F}_q) = 1 + a_1 + a_2 + q a_1 + q^2.$$

2.2 Pairings

It was first observed by Menezes, Okamoto, and Vanstone in [MOV93] that one may be able to reduce the discrete logarithm problem on a curve defined over $\mathbb{F}_q$ to the discrete logarithm in the multiplicative group of a finite field, $\mathbb{F}_{q^k}$ for some k, by means of a pairing on the curve. The DLP in $\mathbb{F}_{q^k}^*$ is amenable to more efficient techniques, such as index calculus methods, thus potentially rendering the curves less secure. The original MOV attack used the Weil pairing, which we do not define here, but as Frey and Rück show in [FR94], one could equally well use the Tate pairing to provide the necessary bilinear non-degenerate map. Since the Tate pairing is less costly from a computational point of view, so we will focus on its use (see Definition 2.2.1).

The reduction procedure is commonly referred to as the *MOV attack* or *Frey-Rück attack*, and it works as follows. Let C be a hyperelliptic curve over $\mathbb{F}_q$ and e be a suitable pairing. Let $P \in J_C(\mathbb{F}_{q^k})$ of order n and $Q \in < P >$. We wish to find an integer α such that $Q = \alpha P$. We find some point $R \in J_C(\mathbb{F}_{q^k})[n]$ such that $g = e(P, R)$ has order n, and compute $h = e(Q, R)$. Since e is non-degenerate, h has order n, and since e is bilinear, we have $h = g^\alpha$.

Thus the DLP on the curve has been reduced to a DLP in the multiplicative group of a finite field.

Now, when given a divisor $D = \sum_{P \in C} n_P P$ of degree zero and a function $f \in \mathbb{F}_q(C)$ such that D and $\mathrm{div}(f)$ have disjoint support, we define $f(D) = \prod_{P \in C, n_P \neq 0} f(P)^{n_P}$.

Definition 2.2.1. Let $\ell > 0$ be an integer prime to q, and let $k \in \mathbb{Z}$ be minimal with $\ell \mid (q^k - 1)$. The *Tate pairing* is a bilinear map

$$T_l : J_C(\mathbb{F}_{q^k})[\ell] \times J_C(\mathbb{F}_{q^k})/\ell J_C(\mathbb{F}_{q^k}) \longrightarrow \mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^\ell$$

defined in the following way [CF05, Section 16.1.1]: Take $P \in J_C(\mathbb{F}_{q^k})[\ell]$ and $Q \in J_C(\mathbb{F}_{q^k})$. Represent P by a divisor D_P of degree 0 defined over $\mathbb{F}_{q^k}$, and let f_P be a function on C with $\mathrm{div}(f_P) = \ell(D_P)$. Represent Q by a divisor D_Q of degree 0 defined over $\mathbb{F}_{q^k}$ such that D_Q and D_P have disjoint support. (One can show that in every divisor class there is a divisor D_Q with support disjoint to D_P, as in [MOV93] and [FMR99].) Then

$$T_\ell(P, Q) = f_P(D_Q) \ \in \mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^\ell.$$

The Tate pairing is usually not symmetric. If $\ell \mid q - 1$ then it is non-degenerate in the sense that for any given $P \in J_C(\mathbb{F}_{q^k})[\ell]$ not equal to O, we can always find a $Q \in J_C(\mathbb{F}_{q^k})$ such that $T_\ell(P, Q) \neq 1$. Instead of taking values of the pairing as classes modulo ℓ-th powers, one usually gets a unique representation by considering the reduced pairing

$$T(P, Q) = f_P(D_Q)^{(q^k-1)/\ell} \in \mu_\ell \subset \mathbb{F}_{q^k}^*.$$

2.3 Embedding degree and security

Since it is possible to embed a subgroup of $J_C(\mathbb{F}_q)$ into $\mathbb{F}_{q^k}^*$, the parameter k has become known as the *embedding degree* and has been viewed as an indicator of the security of the curve.

Definition 2.3.1. A subgroup of $J_C(\mathbb{F}_q)$ with order ℓ has *embedding degree* k *with respect to* ℓ if k is the smallest integer such that $\ell \mid q^k - 1$.

We see that the embedding degree may be viewed as $k = \text{ord}_\ell q$, where $\text{ord}_\ell q$ is defined according to the following definition.

Definition 2.3.2. Let p be a positive integer and ℓ be a prime, $\ell \nmid p$. The smallest positive integer x such that $p^x \equiv 1 \bmod \ell$ is called the *order of* p *modulo* ℓ, denoted by $\text{ord}_\ell p$.

In Chapter 4, we will present examples to show why the embedding degree can be an inaccurate indicator of security, as the pairing can embed into a significantly smaller field than the one suggested by k. The embedding degree k has utility as it indicates the field one must work over to compute the pairing, which needs to be small enough for computations to be efficient. Meanwhile, in security analysis, one would like to compare the difficulty of solving the DLP in the minimal embedding field with solving the DLP on the curve, as both should be computationally intractable [CF05, Section 24.2.2]. Galbraith in [Gal01b] suggests k/g should be considered for security, as this represents the logarithmic ratio between the size of the finite field $\mathbb{F}_{q^k}$ and the size of $J_C(\mathbb{F}_q)$. We follow a terminology ([Sil03]) compatible with [RS02]:

Definition 2.3.3. The *security parameter* with respect to an ℓ-order subgroup of a curve of genus g over a finite field $\mathbb{F}_{p^m}$ is $k' = \frac{\mathrm{ord}_\ell p}{mg}$.

We note that for cryptographic security one needs the size of the minimal embedding field to be of approximately 1024 bits to avoid index calculus computations, and the prime ℓ should be approximately 160 bits so that the DLP on the curve is suitably hard [CF05, Section 24.2.1c]. Thus, the security parameter for an elliptic curve over $\mathbb{F}_p$ in such a case would be approximately 6.

Chapter 3

A Family of Curves

We now consider curves of genus two over $\mathbb{F}_q$, where $q = 2^m$, and whose associated Jacobian is 2-rank 1, neither supersingular, nor ordinary. [LS05] gives formulas for fast arithmetic on genus two curves over binary fields, and [Bir06] gives them for 2-rank 1 curves, which suggests such curves are interesting to consider for cryptosystems.

The fact that there exist simple abelian surfaces with characteristic polynomial of Frobenius $f(t) = t^4 + a_1t^3 + a_2t^2 + qa_1t + q^2 \in \mathbb{Z}[t]$ for certain conditions on a_1 and a_2 is shown in [Rüc90], but that there exists a Jacobian of a curve defined over $\mathbb{F}_q$ with such a characteristic polynomial is due to [MN02]. So we have that (a_1, a_2) determines the $\mathbb{F}_q$-isogeny class of the Jacobian of a smooth projective curve C of genus two defined over $\mathbb{F}_q$, with $\#J_C(\mathbb{F}_q) = q^2 + a_1q + a_2 + a_1 + 1$.

We let C be a curve of genus two over $\mathbb{F}_q$ of the form

$$y^2 + xy = x^5 + bx^3 + cx^2 + dx$$

where $b, c, d \in \mathbb{F}_q^*$, and with characteristic polynomial of Frobenius $f(t) = t^4 + a_1t^3 + a_2t^2 + qa_1t + q^2 \in \mathbb{Z}[t]$. Our approach is as follows. In Section 3.1,

we give a parametrization of a family of large numbers, $N_{r,L} = \frac{2^{2^r L}+1}{2^{2^r}+1}$ for $r \geq 0$ and odd $L \geq 9$, and we determine the embedding degrees for subgroups having these orders when they are prime. In Section 3.2, we associate with each of these primes a sequence of genus two curves over $\mathbb{F}_q$, whose group of $\mathbb{F}_q$-rational points of its Jacobian has order that is divisible by the prime $N_{r,L}$. For example, for each m in the interval $\lceil \frac{2^{r+1}L}{3} \rceil \leq m \leq 2^r(L-1)-1$, we get $\#J_C(\mathbb{F}_q) = 2^x(2^{2^r}+1)N_{r,L}$, where $x = 2m - 2^r L$. We describe the curves by the $\mathbb{F}_q$-isogeny class of their Jacobians, such as having $a_1 = -1$, and $a_2 = 2^m + 2^x$ in the case mentioned above. We show that for our family of curves the ratio ρ is often near 1 and is never more than 2, which suggests efficient implementation would be possible. We give examples of the parameters for such curves with embedding degree $k = 8, 13, 16, 23, 26, 37, 46, 52$. In Section 3.3, we show that the embedding degree k is always "small," that is, $k < (\log q)^2$, so that computations in $\mathbb{F}_{q^k}$ may be feasible.

3.1 Family of primes and their embedding degrees

We consider when $N_{r,L} = \frac{2^{2^r L}+1}{2^{2^r}+1}$ is a prime[1] for some $r \geq 0$ and odd $L \geq 5$. We have seen experimentally that for $r = 0, 2, 3$, $N_{r,L}$ is very often prime. These primes are of the form $\frac{A^L+1}{A+1}$ where L is prime and A is a positive integer; if the behavior follows that of the primes $\frac{A^L-1}{A-1}$ and there is no algebraic factorization, then we would expect there to be infinitely many such primes, and that the number of such primes with $L \leq N$ is asymptotic to $\frac{\log \log N}{\log A}$ for fixed A [Cal06].

[1] $N_{r,L} = 2^{2^r(L-1)} - 2^{2^r(L-2)} + 2^{2^r(L-3)} - 2^{2^r(L-4)} + \cdots - 2 + 1$, so clearly $N_{r,L} \in \mathbb{Z}$ for $r \geq 0$ and odd $L \geq 5$.

Experimental evidence seems to confirm this for $r = 0, 2, 3$.

Our families of curves will be those whose Jacobian is such that its group of $\mathbb{F}_q$-rational points has order divisible by $N_{r,L}$, and whose (a_1, a_2) have a specific description to be explicitly given later.

We must first prove several lemmas that will enable us to achieve our main result. We begin by noting that $r = 1$ never yields a prime.

Lemma 3.1.1. *Let $L \geq 5$ be odd. $N_{1,L} = \frac{2^{2L}+1}{2^2+1}$ is not a prime.*

Proof. Let $P = \frac{2^L+1}{2+1} = N_{0,L}$. We see that $9P^2 = 2^{2L} + 2^{L+1} + 1$. So $N_{1,L} = \frac{9P^2-2^{L+1}}{2^2+1}$. Now L is odd, so $L + 1$ is even. So $N_{1,L} = \frac{(3P-2^{\frac{L+1}{2}})(3P+2^{\frac{L+1}{2}})}{2^2+1}$, and for $L > 1$, each factor is greater than 1. Now $N_{1,L} \in \mathbb{Z}$ and $2^2 + 1$ is prime, so either $(\frac{3P-2^{\frac{L+1}{2}}}{2^2+1}) \in \mathbb{Z}$ or $(\frac{3P+2^{\frac{L+1}{2}}}{2^2+1}) \in \mathbb{Z}$. Since $3P + 2^{\frac{L+1}{2}} = 2^L + 1 + 2^{\frac{L+1}{2}}$ equals 5 only if $L = 1$ and $3P - 2^{\frac{L+1}{2}} = 2^L + 1 - 2^{\frac{L+1}{2}}$ equals 5 only if $L = 3$, then this is a nontrivial factorization when $L \geq 5$. Thus, $N_{1,L}$ is not prime for $L \geq 5$. □

We now determine the embedding degree for a general prime N over $\mathbb{F}_q$.

Lemma 3.1.2. *Let $q = p^m$ for some prime p and positive integer m, N be a prime not equal to p, and k be the smallest positive integer such that $q^k \equiv 1 \bmod N$. Then*

$$k = \frac{\mathrm{ord}_N p}{\gcd(\mathrm{ord}_N p, m)}.$$

Proof. Let $D = \gcd(\text{ord}_N p, m)$. We observe that

$$1 \equiv p^{\text{ord}_N p} \equiv (p^{\text{ord}_N p})^{m/D} \equiv (p^m)^{\text{ord}_N p/D} \bmod N,$$

so since $q = p^m$ and k is the smallest integer such that $q^k \equiv 1 \bmod N$, then we have $k \mid \frac{\text{ord}_N p}{D}$.

We also know that $\text{ord}_N p \mid mk$, and this implies $\frac{\text{ord}_N p}{D} \mid \frac{m}{D}k$. But $\gcd(\frac{\text{ord}_N p}{D}, \frac{m}{D}) = 1$, therefore it must be that $\frac{\text{ord}_N p}{D} \mid k$. Thus we have $k = \frac{\text{ord}_N p}{D}$ and the proof is complete. □

Motivated by this understanding of k, we determine $\text{ord}_{N_{r,L}} 2$ via the following lemmas.

Lemma 3.1.3. *Let $r \geq 0$ and $L \geq 5$ be odd. If $N_{r,L} = \frac{2^{2^r L}+1}{2^{2^r}+1}$ is prime, then L is prime.*

Proof. We first note that if $A = ab$ for positive integers a, b where b is odd, then $x^a + 1 \mid x^A + 1$ for any integer x. To see this:

$$x^A + 1 = x^{ab} + 1 = (x^a + 1)(x^{a(b-1)} - x^{a(b-2)} + x^{a(b-3)} - \cdots + 1).$$

Thus $x^a + 1 \mid x^A + 1$.

Now, if our odd L is not prime, then $L = ab$ for odd $a, b > 1$. By the above argument, $2^{2^r} + 1 \mid 2^{2^r a} + 1$ and $2^{2^r a} + 1 \mid 2^{2^r L} + 1$ imply that $\frac{2^{2^r a}+1}{2^{2^r}+1} \mid \frac{2^{2^r L}+1}{2^{2^r}+1}$. But if $\frac{2^{2^r L}+1}{2^{2^r}+1}$ is prime, then it must be that $a = L$, and hence L is prime. □

Lemma 3.1.4. *Let $r \geq 0$ and $L \geq 5$ be odd. If $N_{r,L} = \frac{2^{2^r L}+1}{2^{2^r}+1}$ is prime, then $\text{ord}_{N_{r,L}} 2 = 2^{r+1} L$.*

Proof. We have $(2^{2^r}+1)N_{r,L} = 2^{2^r L}+1$. So $2^{2^r L} \equiv -1 \bmod N_{r,L}$. This implies $2^{2^{r+1}L} \equiv 1 \bmod N_{r,L}$. So $\mathrm{ord}_{N_{r,L}} 2 \mid 2^{r+1}L$. But by Lemma 3.1.3 we know that L is prime, so it must be that either $\mathrm{ord}_{N_{r,L}} 2 = 2^j$ or $\mathrm{ord}_{N_{r,L}} 2 = 2^j L$ for some $0 \leq j \leq r+1$.

Suppose $\mathrm{ord}_{N_{r,L}} 2 = 2^j$ for some $0 \leq j \leq r+1$. Then $2^{2^j} \equiv 1 \bmod N_{r,L}$. So $N_{r,L} \mid 2^{2^j} - 1$. This implies $N_{r,L} \leq 2^{2^j} - 1 \leq 2^{2^{r+1}} - 1$. But we know that $N_{r,L} > 2^{2^r(L-2)} \geq 2^{2^r 3} > 2^{2^{r+1}} - 1$ for $L \geq 5$. Therefore, $\mathrm{ord}_{N_{r,L}} 2 \neq 2^j$ for $0 \leq j \leq r+1$.

Now suppose $\mathrm{ord}_{N_{r,L}} 2 = 2^j L$ for some $0 \leq j \leq r$. Then

$$\begin{aligned} 2^{2^j L} \equiv 1 \bmod N_{r,L} &\Rightarrow (2^{2^j L})^{2^{r-j}} \equiv 1 \bmod N_{r,L} \\ &\Rightarrow 2^{2^r L} \equiv 1 \bmod N_{r,L}. \end{aligned}$$

But we know that $2^{2^r L} \equiv -1 \bmod N_{r,L}$. Thus it must be that $j = r+1$ and so $\mathrm{ord}_{N_{r,L}} 2 = 2^{r+1}L$. □

We are now able to state the embedding degree k of a group of order $N_{r,L}$, where $q = 2^m$ for a specific range of m. Here we study the traditional embedding degree k; however, in Chapter 4, we will revisit this understanding and consider a separate security parameter that indicates the minimal embedding field.

Lemma 3.1.5. *Let $N_{r,L} = \frac{2^{2^r L}+1}{2^{2^r}+1}$ be prime for some $r \geq 0$ and odd $L \geq 5$, $m \leq 2^r(L-1) - 1$ and also allow $m = \frac{L+1}{2}$ in the case that $r = 0$, and let k be the embedding degree of curve C with respect to $N_{r,L}$. Then $k = 2^{r+1-i}$*

when $\gcd(\mathrm{ord}_{N_{r,L}}2, m) = 2^i L$ *for* $i \in \{0, \ldots, r-1\}$*, and* $k = 2^{r+1-i}L$ *when* $\gcd(\mathrm{ord}_{N_{r,L}}2, m) = 2^i$ *for* $i \in \{0, \ldots, r+1\}$.

Proof. By Lemma 3.1.4, we know that $\mathrm{ord}_{N_{r,L}}2 = 2^{r+1}L$. Suppose $\gcd(\mathrm{ord}_{N_{r,L}}2, m) = 2^i L$ for $0 \leq i \leq r-1$. (Note that $i \leq r-1$ since $\gcd(\mathrm{ord}_{N_{r,L}}2, m) = 2^i L \leq m \leq 2^r(L-1) - 1$.) Then by Lemma 3.1.2,

$$k = \frac{\mathrm{ord}_{N_{r,L}}2}{\gcd(\mathrm{ord}_{N_{r,L}}2, m)} = \frac{2^{r+1}L}{2^i L} = 2^{r+1-i}.$$

Now suppose $\gcd(\mathrm{ord}_{N_{r,L}}2, m) = 2^i$ for $0 \leq i \leq r+1$. Then

$$k = \frac{\mathrm{ord}_{N_{r,L}}2}{\gcd(\mathrm{ord}_{N_{r,L}}2, m)} = \frac{2^{r+1}L}{2^i} = 2^{r+1-i}L.$$

(Note that since $\frac{2^{r+1}L}{2^i} \in \mathbb{Z}$ and L is odd, then $i \leq r+1$.) □

We note that the embedding degree k is unbounded as L is unbounded. We now seek to find curves over $\mathbb{F}_q$ associated with Jacobians whose group of $\mathbb{F}_q$-rational points has order is divisible by $N_{r,L}$.

3.2 Genus 2 curves for a given $\mathbb{F}_q$-isogeny class of Jacobians

We know that the (a_1, a_2) determines the $\mathbb{F}_q$-isogeny class of the Jacobian of a curve of genus two, and the following theorem is a consequence of [MN02] and gives the conditions for a curve associated with such a Jacobian to exist. A converse is also proven in [MN02], but we will not need it for our result. (This statement combines Lemma 2.1, Theorem 2.9 part (M) and Corollary 2.17 of [MN02], as it appears in [MV05].)

Theorem 3.2.1. *Let $q = p^m$ for a prime p and positive integer m. There exists a curve of the form $y^2 + xy = x^5 + bx^3 + cx^2 + dx$, $b, c, d \in \mathbb{F}_q^*$, with characteristic polynomial of Frobenius $f(t) = t^4 + a_1t^3 + a_2t^2 + qa_1t + q^2$ if the following conditions hold:*

1. *a_1 is odd,*
2. *$|a_1| \leq 4\sqrt{q}$,*
3. *there exists an integer a_2 such that*
   - *(a) $2|a_1|\sqrt{q} - 2q \leq a_2 \leq a_1^2/4 + 2q$,*
   - *(b) a_2 is divisible by $2^{\lceil m/2 \rceil}$,*
   - *(c) $\Delta = a_1^2 - 4a_2 + 8q$ is not a square in $\mathbb{Z}$,*
   - *(d) $\delta = (a_2 + 2q)^2 - 4qa_1^2$ is not a square in $\mathbb{Z}_2$ (the 2-adic integers).*

We use this theorem to establish the existence of curves of genus two with specific conditions on (a_1, a_2). We then show these are the conditions needed so that $\#J_C(\mathbb{F}_q)$ is divisible by $N_{r,L}$.

We first give a lemma that will be used in the proof of the next proposition.

Lemma 3.2.2. *If a, b, c are integers, with $a, b > 0$, and $2^a(2^b - 1) = c(c + 1)$ then $a \leq b$.*

Proof. Suppose c is even. Then $c+1$ is odd. So $2^a \mid c$, and $c = 2^a x$ for some odd integer x such that $|x| \geq 1$, and $x(c+1) = 2^b - 1$. Then $2^b = x(2^a x + 1) + 1$. If $x \geq 1$, then $2^b \geq 2^a + 2$ and so $b > a$. If $x \leq 1$, then $2^b = |x|(2^a|x| - 1) + 1 \geq 2^a$ and so $b \geq a$.

Now suppose $c+1$ is even. Then c is odd. So $2^a \mid c+1$ and $c+1 = 2^a x$ for some odd integer x such that $|x| \geq 1$ and $xc = 2^b - 1$. Then $2^b = x(2^a x - 1) + 1$. If $x \geq 1$, then $2^b \geq 2^a$, and so $b \geq a$. If $x \leq 1$, then $2^b = |x|(2^a|x| + 1) + 1 \geq 2^a + 2$, and so $b > a$. □

Proposition 3.2.3. *Let $q = 2^m$, $r \geq 0$ and $L \geq 9$ be prime. When $m = \frac{L+1}{2}$, let $a_1 = 1$ and $a_2 = -2^m$, and when $\lceil \frac{2^{r+1}L}{3} \rceil \leq m \leq 2^r(L-1) - 1$, let $a_1 = -1$ and $a_2 = 2^m + 2^{2m-2^r L}$. These a_1 and a_2 satisfy the conditions for the existence of the curves of genus two in Theorem 3.2.1.*

Proof. We first note that since $L \geq 9$, then $m = \frac{L+1}{2} \geq 5$. Now, clearly a_1 is odd and $|a_1| \leq 4\sqrt{q}$ in both cases of the proposition.

Let us show $2|a_1|\sqrt{q} - 2q \leq a_2 \leq a_1^2/4 + 2q$. The first case (when $a_1 = 1$ and $a_2 = -q$ for $m = \frac{L+1}{2}$), gives $2\sqrt{q} - 2q \leq -q \leq 1/4 + 2q$, which is true for $L \geq 9$. Now consider the second case (when $a_1 = -1$, and $a_2 = 2^m + 2^{2m-2^r L}$):

$$2\sqrt{q} - 2q \leq a_2 \leq 1/4 + 2q$$

$$\iff 2^{m/2+1} - 2^{m+1} \leq 2^m + 2^{2m-2^r L} \leq 1/4 + 2^{m+1}.$$

Clearly the first inequality holds. The second inequality holds if $2^{2m-2^r L} \leq 2^m$, which holds if $m \leq 2^r L$. This is true since $m \leq 2^r(L-1) - 1$.

Let us show $2^{\lceil m/2 \rceil} \mid a_2$. Clearly the first case is true: $2^{\lceil m/2 \rceil} \mid -2^m$. Now consider the second case:

$$2^{\lceil m/2 \rceil} \mid 2^m + 2^{2m-2^r L}$$

$$\iff 2m - 2^r L \geq \lceil m/2 \rceil$$

$$\iff \lfloor 3m/2 \rfloor \geq 2^r L$$
$$\iff m \geq \lceil \frac{2^{r+1}L}{3} \rceil.$$

Thus the condition holds.

Now we show $\Delta = a_1^2 - 4a_2 + 8q$ is not a square in $\mathbb{Z}$. The first case yields $\Delta = 1 + 3 \cdot 2^{m+2}$. Suppose $\Delta = 1 + 3 \cdot 2^{m+2} = x^2$ for some integer x. Since $1 + 3 \cdot 2^{m+2}$ is odd, then x is odd, so let $x = 2c + 1$ for some integer c. Then Δ is a square if and only if $3 \cdot 2^m = 2^m(2^2 - 1) = c(c + 1)$. We apply Lemma 3.2.2, letting $a = m$ and $b = 2$. Then Δ is a square implies $m \leq 2$. Thus Δ is not a square in $\mathbb{Z}$ for $m = \frac{L+1}{2}$, since $m \geq 5$ for $L \geq 9$. The second case yields $\Delta = 2^{2m-2^r L+2}(2^{2^r L-m} - 1) + 1$. For contradiction, suppose $\Delta = 2^{2m-2^r L+2}(2^{2^r L-m} - 1) + 1 = x^2$ for some integer x. Since Δ is odd, then x is odd, so let $x = 2c+1$ for some integer c. Then Δ is a square if and only if $2^{2m-2^r L}(2^{2^r L-m} - 1) = c(c+1)$. We apply Lemma 3.2.2, letting $a = 2m - 2^r L$ and $b = 2^r L - m$. We note that $a > 0$ since $m \geq \lceil \frac{2^{r+1}L}{3} \rceil$ implies $\lfloor \frac{3m}{2} \rfloor \geq 2^r L$, and so $2m - 2^r L > 0$. Also $b > 0$ since $m \leq 2^r(L - 1) - 1$ implies $m \leq 2^r L$, and so $2^r L - m > 0$. Thus Δ a square implies $2m - 2^r L \leq 2^r L - m$, that is, $m \leq \frac{2^{r+1}L}{3}$. Since L is prime and $L \neq 3$, then $\frac{2^{r+1}L}{3} \notin \mathbb{Z}$, so in fact we have $m \leq \lfloor \frac{2^{r+1}L}{3} \rfloor < \lceil \frac{2^{r+1}L}{3} \rceil$. But we know that $\lceil \frac{2^{r+1}L}{3} \rceil \leq m$, so this will not hold, and hence Δ is not a square.

Now we show $\delta = (a_2+2q)^2 - 4qa_1^2$ is not a square in the 2-adic integers, $\mathbb{Z}_2$. That is, for $\delta = 2^x b$, we must show that either $b \not\equiv 1 \bmod 8$ or $x \equiv 1 \bmod 2$. The first case yields $\delta = q^2 - 4q = 2^{m+2}(2^{m-2} - 1)$. So $b = 2^{m-2} - 1 \equiv -1 \bmod 8$ for $m \geq 5$. Therefore δ is not a square in $\mathbb{Z}_2$ for $m = \frac{L+1}{2}$, since $m \geq 5$ when

$L \geq 9$.

Now consider the second case:

$$\delta = (2^m + 2^{2m-2^rL} + 2^{m+1})^2 - 2^{m+2}$$

$$= (2^m + 2^{2m-2^rL})^2 + 2^{m+2}(2^m + 2^{2m-2^rL}) + 2^{2m+2} - 2^{m+2}$$

$$= 2^{2m+3} + 2^{2m} + 2^{3m-2^rL+2} + 2^{3m-2^rL+1} + 2^{4m-2^{r+1}L} - 2^{m+2}$$

$$= 2^{m+2}(2^{m+1} + 2^{m-2} + 2^{2m-2^rL} + 2^{2m-2^rL-1} + 2^{3m-2^rL-2} - 1)$$

$$\Rightarrow b = 2^{m-2}(2^3 + 1) + 2^{2m-2^rL-1}(2 + 1) + 2^{3m-2^{r+1}L-2} - 1.$$

For $m \geq 5$, we have

$$\begin{aligned} b &\equiv 2^{2m-2^rL-1}(3) + 2^{3m-2^{r+1}L-2} - 1 \bmod 8 \\ &\equiv 2^{3m-2^{r+1}L-2}(2^{2^rL-m+1}3 + 1) - 1 \bmod 8. \end{aligned}$$

Now, suppose $b \equiv 1 \bmod 8$. Then

$$b + 1 \equiv 2^{3m-2^{r+1}L-2}(2^{2^rL-m+1}3 + 1) \equiv 2 \bmod 8.$$

Clearly $3m-2^{r+1}L-2$ cannot be greater than or equal to 3. Now if $3m-2^{r+1}L-2 = 2$, then we have $4(2^{2^rL-m+1}3 + 1) \equiv 2 \bmod 8$. But a multiple of 4 cannot be congruent to 2 modulo 8, so this cannot happen. If $3m - 2^{r+1}L - 2 = 1$, then $m = \frac{3+2^{r+1}L}{3}$. But L is prime and $L \neq 3$, so $m \notin \mathbb{Z}$, and this cannot happen as we require an integer m. If $3m - 2^{r+1}L - 2 = 0$, then we have $2^{2^rL-m+1}3 + 1 \equiv 2 \bmod 8$. But an odd number cannot be congruent to 2 modulo 8, so this cannot happen. Thus $b \not\equiv 1 \bmod 8$, and so δ is not a square in $\mathbb{Z}_2$.

Therefore all the conditions for the existence of genus 2 curves C over $\mathbb{F}_q$ are satisfied for the given (a_1, a_2) described in the proposition. $\square$

We are now able to state our main result in the following theorem.

Theorem 3.2.4. *Let $N_{r,L} = \frac{2^{2^r L}+1}{2^{2^r}+1}$ be a prime for some $r \geq 0$ and odd $L \geq 9$. If $r = 0$, then for $m = \frac{L+1}{2}$ there exists a curve C of genus two over $\mathbb{F}_{2^m}$ with the property that $\#J_C(\mathbb{F}_{2^m}) = 2 \cdot 3 \cdot N_{0,L}$, and $a_1 = 1, a_2 = -2^m$. If $r \geq 0$, then for each integer m in the interval $\lceil \frac{2^{r+1}L}{3} \rceil \leq m \leq 2^r(L-1) - 1$, there exists a curve C of genus two over $\mathbb{F}_{2^m}$ with the property that $\#J_C(\mathbb{F}_{2^m}) = 2^x(2^{2^r}+1)N_{r,L}$, where $x = 2m - 2^r L$, and $a_1 = -1, a_2 = 2^m + 2^x$.*

Proof. Let $N_{r,L} = \frac{2^{2^r L}+1}{2^{2^r}+1}$ be a prime for some $r \geq 0$ and odd $L \geq 9$.

We know by Proposition 3.2.3, that the (a_1, a_2) stated in the theorem, with m in the specified range, satisfy the conditions for the existence of a curve C of genus 2 over $\mathbb{F}_{2^m}$. We now examine $\#J_C(\mathbb{F}_q)$, recalling that $\#J_C(\mathbb{F}_q) = q^2 + a_1 q + a_2 + a_1 + 1$.

First we consider when $r = 0$ and $m = \frac{L+1}{2}$. For $a_1 = 1$ and $a_2 = -2^m$, we have

$$\#J_C(\mathbb{F}_{2^m}) = 2^{2m} + 2^m - 2^m + 2 = 2^{2m} + 2.$$

Since $m = \frac{L+1}{2}$, we have $L = 2m - 1$, so

$$\begin{aligned} \#J_C(\mathbb{F}_{2^m}) = 2^{L+1} + 2 &= 2(2^L + 1) \\ &= 2 \cdot 3 \cdot N_{0,L} \text{ since } N_{0,L} = \frac{2^L + 1}{2 + 1}. \end{aligned}$$

Now we consider when $r \geq 0$ is an integer not equal to 1, and $\lceil \frac{2^{r+1}L}{3} \rceil \leq m \leq 2^r(L-1)-1$. For $a_1 = -1$ and $a_2 = 2^m + 2^x$, where $x = 2m - 2^r L$, we have

$$\begin{aligned} \#J_C(\mathbb{F}_{2^m}) = 2^{2m} - 2^m + 2^m + 2^x &= 2^{2m} + 2^x \\ &= 2^x(2^{2^r L} + 1) \\ &= 2^x(2^{2^r} + 1)N_{r,L} \text{ since } N_{r,L} = \frac{2^{2^r L}+1}{2^{2^r}+1}. \end{aligned}$$

Thus the theorem is complete. □

Now let $\#J_C(\mathbb{F}_q) = hN_{r,L}$. For the most efficient implementation of a pairing-based cryptosystem, we would like the cofactor h to be small, that is, for the ratio $\rho = \frac{2\log_2 q}{\log_2 N_{r,L}}$ to be approximately 1. For our family of curves, we see that $\rho \sim \frac{m}{2^{r-1}(L-1)}$, which is often near 1 and at most 2. In particular, when $m = \frac{L+1}{2}$, we get $\rho \sim \frac{L+1}{L-1}$. When $\lceil \frac{2^{r+1}L}{3} \rceil \leq m \leq 2^r(L-1)-1$, the ratio can be as small as $\rho \sim \frac{4L}{3(L-1)}$ and at most $\rho \sim 2 - \frac{2}{2^r(L-1)}$.

Table 3.1 gives some examples of the parameters for curves over $\mathbb{F}_q$ yielding small embedding degrees $k = 8, 13, 16, 23, 26, 37, 46, 52$. A systematic way of determining the explicit coefficients of a curve when given the (a_1, a_2) parameters that distinguish the $\mathbb{F}_q$-isogeny class of its Jacobian is not yet established. As such, in Example 3.2.5 we have used brute force with MAGMA code to generate some examples of these curves over small $\mathbb{F}_q$.

Example 3.2.5. *We give examples over small $\mathbb{F}_q$ for $r = 0$. We let g be a primitive element of $\mathbb{F}_q$.*

$$L = 11,\ m = \tfrac{L+1}{2} = 6,\ k = 11,\ \rho \sim 6/5,$$
$$C : y^2 + xy = x^5 + g^8x^3 + g^3x^2 + gx,$$

$$L = 11,\ m = \lceil \tfrac{2^{r+1}L}{3} \rceil = 8,\ k = 11,\ \rho \sim 8/5,$$
$$C : y^2 + xy = x^5 + g^7x^3 + g^7x$$

$$L = 11,\ m = 2^r(L-1) - 1 = 9,\ k = 22,\ \rho \sim 9/5,$$
$$C : y^2 + xy = x^5 + g^8x^3 + g^3x$$

$$L = 13,\ m = \tfrac{L+1}{2} = 7,\ k = 26,\ \rho \sim 7/6,$$
$$C : y^2 + xy = x^5 + g^{92}x^3 + g^7x^2 + gx$$

$$L = 17,\ m = \tfrac{L+1}{2} = 9,\ k = 34,\ \rho \sim 9/8,$$
$$C : y^2 + xy = x^5 + g^{103}x^3 + g^5x^2 + gx$$

3.3 Size of the embedding degrees

We examine the size of the embedding degrees of the family of curves from Theorem 3.2.4. We find that for cryptographic sizes, these curves always yield embedding degrees such that $k < (\log\ q)^2$, which suggests that the embedding degree may be small enough so that computations are feasible. (See [BK98] and [GM05, Section 5.2.1] for discussion of the probability of k in this range.)

Proposition 3.3.1. *Let $q = 2^m$, $N_{r,L} = \frac{2^{2^r L}+1}{2^{2^r}+1}$ be prime for some $r \geq 0$ and odd $L \geq 5$, and k be the embedding degree of curve C with respect to $N_{r,L}$. If*

k	L	r	m	a_1	a_2	ρ
8	37	2	111	-1	$2^{111}+2^{74}$	3/2
8	89	2	267	-1	$2^{267}+2^{178}$	3/2
8	149	2	447	-1	$2^{447}+2^{298}$	3/2
13	13	3	80	-1	$2^{80}+2^{56}$	5/3
16	13	3	91	-1	$2^{91}+2^{78}$	2
23	23	2	64	-1	$2^{64}+2^{36}$	3/2
23	23	2	72	-1	$2^{72}+2^{52}$	5/3
23	23	2	80	-1	$2^{80}+2^{68}$	9/5
26	13	3	72	-1	$2^{72}+2^{40}$	3/2
26	13	3	88	-1	$2^{88}+2^{72}$	9/5
37	37	2	104	-1	$2^{104}+2^{60}$	7/5
37	37	2	112	-1	$2^{112}+2^{76}$	3/2
37	37	2	120	-1	$2^{120}+2^{92}$	5/3
37	37	2	128	-1	$2^{128}+2^{108}$	9/5
37	37	2	136	-1	$2^{136}+2^{124}$	2
46	23	2	68	-1	$2^{68}+2^{44}$	3/2
46	23	2	76	-1	$2^{76}+2^{60}$	7/4
46	23	2	84	-1	$2^{84}+2^{76}$	2
52	13	3	76	-1	$2^{76}+2^{48}$	5/3
52	13	3	88	-1	$2^{88}+2^{64}$	7/4
52	13	3	92	-1	$2^{92}+2^{80}$	2

Table 3.1: Examples of parameters for families of genus 2 curves over $\mathbb{F}_{2^m}$ with small embedding degree k.

$L \geq 11$, then for each integer m in the interval $\lceil \frac{2^{r+1}L}{3} \rceil \leq m \leq 2^r(L-1)-1$, $k < (\log\ q)^2$. If $L \geq 15$, then when $r = 0$ and $m = \frac{L+1}{2}$, $k < (\log\ q)^2$.

Proof. Let $\lceil \frac{2^{r+1}L}{3} \rceil \leq m \leq 2^r(L-1)-1$. By Lemma 3.1.5, the largest that k can be is $k = 2^{r+1}L$, so it suffices to consider this case. Given the acceptable range

for m, it is enough to show $k < (\log\ q)^2$ for $m = \lceil \frac{2^{r+1}L}{3} \rceil$. Now $k < (\log\ q)^2$ if

$$\begin{aligned} 2^{r+1}L &< (\log\ 2^{\frac{2^{r+1}L}{3}})^2 \\ 2^{r+1}L &< (\frac{2^{r+1}L}{3})^2(\log^2 2) \\ 9 \cdot 2^{r+1}L &< 2^{2r+2}(\log^2 2)L^2 \\ \frac{9}{2^{r+1}(\log^2 2)} &< L. \end{aligned}$$

This holds if $L \geq 10$ for $r = 0$. Since we require L to be odd, we can say that $L \geq 11$ for any $r \geq 0$ gives the result.

Now let $m = \frac{L+1}{2}$ and $r = 0$. By Lemma 3.1.5, it suffices to consider $k = 2L$. Now $k < (\log\ q)^2$ if

$$\begin{aligned} 2L &< (\log\ 2^{(L+1)/2})^2 \\ 2L &< (\frac{L+1}{2})^2(\log^2 2) \\ 2(L+1) - 2 &< \frac{\log^2 2}{4}(L+1)^2 \\ 0 &< \frac{\log^2 2}{4}(L+1)^2 - 2(L+1) + 2. \end{aligned}$$

This holds if $L + 1 > \frac{2+\sqrt{4-2(\log^2 2)}}{\frac{\log^2 2}{2}}$, that is, if $L \geq 15$. □

Chapter 4

Minimal Embedding Field

As mentioned in the previous chapters, pairing-based attacks can transport the discrete logarithm problem in $J_C(\mathbb{F}_q)$ to the discrete logarithm in the multiplicative group of a finite field, where there are more efficient methods for solving the DLP. Such attacks have traditionally been viewed as mapping the DLP into the smallest extension of $\mathbb{F}_q$ that contains the ℓ-th roots of unity, where ℓ is the order of a subgroup of $J_C(\mathbb{F}_q)$; that is, $\mathbb{F}_q(\mu_\ell) = \mathbb{F}_{q^k}$ for some integer k.

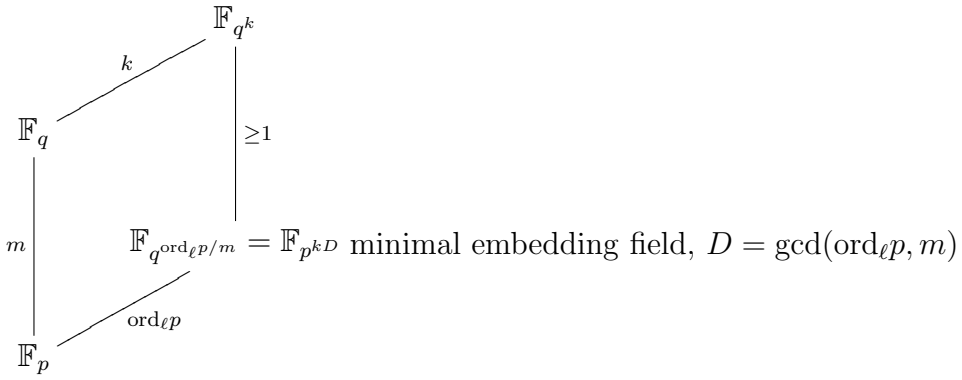
We construct examples to demonstrate that the minimal field containing the embedding, i.e., the smallest extension of $\mathbb{F}_p$ containing the ℓ-th roots of unity, can be a significantly smaller field than $\mathbb{F}_{q^k}$. This can dramatically speed up attacks on the DLP and has the implication that there could be "pairing-friendly" curves that may not be as secure as previously believed.

In [RS02] it is shown that if A is a simple supersingular abelian variety and ℓ is sufficiently large (compared to $q^{\dim(A)}$), then the extension degree can differ by a factor of at most two with that of $\mathbb{F}_{q^k}$. We provide examples that are not limited to the supersingular case, showing that for curves over

$\mathbb{F}_{p^m}$ of any genus, the extension degrees can differ by as much as a factor of m. This phenomenon only creates a discrepancy in non-prime fields of small characteristic.

4.1 Examination of the minimal embedding field

We recall Lemma 3.1.2, which tells us that for a subgroup of $J_C(\mathbb{F}_q)$ with prime order ℓ, where ℓ does not equal to p, $k = \frac{\mathrm{ord}_\ell p}{\gcd(\mathrm{ord}_\ell p, m)}$. Since μ_ℓ lies in $\mathbb{F}^*_{p^{\mathrm{ord}_\ell p}}$, it is apparent that the minimal embedding field is not $\mathbb{F}_{q^k} = \mathbb{F}_{p^{km}}$, but $\mathbb{F}_{p^{\mathrm{ord}_\ell p}} = \mathbb{F}_{p^{kD}}$, where $D = \gcd(\mathrm{ord}_\ell p, m)$. So it is conceivable for $\mathbb{F}_{q^k}$ and the minimal embedding field to have extension degrees that differ by a factor of m, which can be quite large.



One can potentially make this gap arbitrarily large, simply by increasing the exponent m prime to $\mathrm{ord}_\ell p$. We note that whenever q is prime, there is no difference between the minimal embedding field and $\mathbb{F}_{q^k}$.

To examine the potential difference between the size of the minimal field that contains the embedding and $\mathbb{F}_{q^k}$, let $q = p^m$ with $m \neq 1$, and

let us consider $[\mathbb{F}_{q^k} : \mathbb{F}_{p^{\mathrm{ord}_\ell p}}]$. That is, set $\Delta = \frac{m}{\gcd(\mathrm{ord}_\ell p, m)}$, so the size of Δ reveals the relative change in field size. We see that $\Delta = 1$ if and only if $\gcd(\mathrm{ord}_\ell p, m) = m$, which corresponds to k being an accurate indicator of the minimal embedding field. However, it is not unusual to have $\gcd(\mathrm{ord}_\ell p, m) = 1$, hence $\Delta = m$, showing k to be the least accurate indicator of the minimal embedding field.

4.2 Examples

Let us look at some examples of genus one and genus two curves that emphasize this difference between the size of the minimal embedding field and the field suggested by the embedding degree k. Since cryptographic applications usually focus on prime fields and binary fields, and the discrepancy is only visible in the extension field case, we will give examples in characteristic two.

4.2.1 Elliptic curves

Example 4.2.1. *Consider the Mersenne prime $\ell = 2^p - 1$, let $q = 2^{p+1}$. We know from [WM71] that there exists at least one ordinary elliptic curve over $\mathbb{F}_q$ with $|E(\mathbb{F}_q)| = 2\ell$. This curve has embedding degree $k = p$, so $\mathbb{F}_{q^k} = \mathbb{F}_{2^{p(p+1)}}$. But $\gcd(\mathrm{ord}_\ell 2, p+1) = 1$, so the embedding field is $\mathbb{F}_{2^p}$, and these sizes differ by a factor of $\Delta = p+1$. We note that in this case $\mathbb{F}_{q^k}$ grows quadratically in p, but the minimal embedding field grows only linearly in p.*

Curves in Example 4.2.1 might be discarded since the field exponent is not prime and thus Weil descent attacks might apply. We now show how this

example can be generalized to work with more general exponents.

Example 4.2.2. *Let $\ell = 2^p - 1$ be prime, and $q = 2^{p+s}$, for $1 \leq s \leq p+1$, $s \neq p$. Then we know from [WM71] that for each s there exists at least one ordinary elliptic curve over $\mathbb{F}_q$ with $|E(\mathbb{F}_q)| = 2^s\ell$. We emphasize that this allows for the extension degree to be prime. These curves have embedding degree $k = p$, so $\mathbb{F}_{q^k} = \mathbb{F}_{2^{p(p+s)}}$. But $\gcd(\mathrm{ord}_\ell 2, p+s) = 1$, so the minimal embedding field is $\mathbb{F}_{2^p}$, and these sizes differ by a factor of $\Delta = p + s$.*

4.2.2 Hyperelliptic curves

Example 4.2.3. *We can consider the Mersenne prime $\ell = 2^p - 1$ for genus two curves, which will be more thoroughly presented in Section 4.2.4. We note that these examples have an absolutely simple Jacobian, so these curves are not merely the product of an elliptic curve from Example 4.2.2 and another elliptic curve. For each $\lceil \frac{2p}{3} \rceil \leq m \leq p - 1$, we show in Proposition 4.2.7 that there exists a genus 2 curve C over $\mathbb{F}_{2^m}$ with $\#J_C(\mathbb{F}_{2^m}) = 2^{2m-p}\ell$. Each curve is given by the characteristic polynomial of Frobenius with coefficients $(a_1, a_2) = (-1, 2^m - 2^{2m-p})$. These curves have embedding degree $k = p$, so $\mathbb{F}_{q^k} = \mathbb{F}_{2^{pm}}$, but the minimal embedding field is $\mathbb{F}_{2^p}$, since $\gcd(\mathrm{ord}_\ell 2, m) = 1$.*

We have also checked the accuracy of k as a security parameter in curve examples in the published literature, and the following is a proposed system in [GMV04] which is subject to this discrepancy.

Example 4.2.4. *[from published literature] The authors of [GMV04] propose a family of curves of genus two over $\mathbb{F}_q$ where $q(\ell) = \ell^2$ for any prime (power)*

ℓ. The associated Jacobian defined over $\mathbb{F}_q$ has size $n(\ell) = \ell^4 \pm \ell^3 + \ell^2 \pm \ell + 1$. A prime N dividing $n(\ell)$ clearly divides $q^5 - 1$, but cannot divide $q^k - 1$ for $k < 5$ except in the absurdly small case of $N = 5$. So every curve of this form has embedding degree $k = 5$, as shown in [GMV04, Section 7.3]. However, if $n(\ell) = \ell^4 + \ell^3 + \ell^2 + \ell + 1$, then N divides $\ell^5 - 1 = q^{5/2} - 1$, so in fact the minimal embedding field cannot be larger than $\mathbb{F}_{q^{5/2}}$. This makes a dramatic difference in how large ℓ has to be chosen for the curves to remain secure against pairing-based attacks. However no such security warning is present in [GMV04].

As we have mentioned, whenever working over $\mathbb{F}_q$, for q a prime, there is no discrepancy between the computational and security-related notions of embedding degree, but when q is a prime power there may be a significant difference. The techniques given in [GMV04] mentioned in our Example 4.2.4 are presented in general for prime powers q, although most of the curve examples they list are over a prime field, and hence escape the discrepancy. One should be cautious when using these techniques to generate curves, as certain parameters within a family may yield a prime power q, and hence the curves could be insecure.

We now give two numerical examples taken from the family of curves given in Chapter 3. Though these curves are not used in practice, they serve to illustrate the phenomenon we are examining.

Example 4.2.5. *Consider the genus 2 curve C over $\mathbb{F}_{2^{267}}$ given by the characteristic polynomial of Frobenius with coefficients $(a_1, a_2) = (-1, 2^{267} + 2^{178})$.*

By Theorem 3.2.4, $\#J_C(\mathbb{F}_{2^{267}}) = 2^{178} \cdot 17 \cdot \ell$*, where* $\ell = \frac{2^{4(89)}+1}{17}$ *is prime, and the embedding degree is* $k = 8$*. Since* $\log_2 \ell = 351$ *and* $k \log_2 q = 2136$*, we have a 351-bit DLP on the curve, and a* 2136*-bit DLP in* $\mathbb{F}^*_{q^k}$*, which is considered hard. However, since* $\mathrm{ord}_\ell 2 = mgk' = 712$*, then in the minimal embedding field we have only a* 712*-bit DLP, which is considered easy.*

Example 4.2.6. *Consider the genus 2 curve* C *over* $\mathbb{F}_{2^{136}}$ *given by the characteristic polynomial of Frobenius with coefficients* $(a_1, a_2) = (-1, 2^{136} + 2^{124})$*. By Theorem 3.2.4* $\#J_C(\mathbb{F}_{2^{136}}) = 2^{124} \cdot 17 \cdot \ell$*, where* $\ell = \frac{2^{4(37)}+1}{17}$ *is prime, and the embedding degree is* $k = 37$*. Since* $k \log_2 q = 5032$*, we have a 5032-bit DLP in* $\mathbb{F}^*_{q^k}$*, which is considered hard. However, since* $\mathrm{ord}_\ell 2 = 296$*, then in the minimal embedding field we have only a 296-bit DLP, which is considered easy.*

4.2.3 Family of curves revisited

We revisit the family of curves presented in Chapter 3, and now we not only consider the embedding degree k, but also the security parameter k'. Table 4.1 gives the examples of our curves with the sizes (in bits) of the field $\mathbb{F}_{q^k}$ and the prime-order subgroup, along with mgk', thus providing a more accurate security comparison between the DLP on the curve and in the finite field.

We recall that the difficulty of solving a DLP in a subgroup of prime 160-bit order on a hyperelliptic curve is roughly equivalent to solving a DLP in a finite field of around 1024-bits. As security increases, one has the respective correspondence of the DLP on the curve and in the finite field as being approximately 256-bits to 3072-bits and 512-bits to 15360-bits [GPS06, Table

2]. We present the numerical data in Table 4.1, recognizing that for some of these examples, the DLP on the curve is easy, so the difficulty of the DLP in the finite field is irrelevant.

k	L	r	m	a_1	a_2	$\log_2 N_{r,L}$	$k \log_2 q$	mgk'
8	37	2	111	-1	$2^{111} + 2^{74}$	143	888	296
8	89	2	267	-1	$2^{267} + 2^{178}$	351	2136	712
8	149	2	447	-1	$2^{447} + 2^{298}$	591	3576	1192
13	13	3	80	-1	$2^{80} + 2^{56}$	95	1040	208
16	13	3	91	-1	$2^{91} + 2^{78}$	95	1456	208
23	23	2	64	-1	$2^{64} + 2^{36}$	87	1472	184
23	23	2	72	-1	$2^{72} + 2^{52}$	87	1656	184
23	23	2	80	-1	$2^{80} + 2^{68}$	87	1840	184
26	13	3	72	-1	$2^{72} + 2^{40}$	95	1872	208
26	13	3	88	-1	$2^{88} + 2^{72}$	95	2288	208
37	37	2	104	-1	$2^{104} + 2^{60}$	143	3848	296
37	37	2	112	-1	$2^{112} + 2^{76}$	143	4144	296
37	37	2	120	-1	$2^{120} + 2^{92}$	143	4440	296
37	37	2	128	-1	$2^{128} + 2^{108}$	143	4736	296
37	37	2	136	-1	$2^{136} + 2^{124}$	143	5032	296
46	23	2	68	-1	$2^{68} + 2^{44}$	87	3128	184
46	23	2	76	-1	$2^{76} + 2^{60}$	87	3496	184
46	23	2	84	-1	$2^{84} + 2^{76}$	87	3864	184
52	13	3	76	-1	$2^{76} + 2^{48}$	95	3952	208
52	13	3	88	-1	$2^{88} + 2^{64}$	95	4368	208
52	13	3	92	-1	$2^{92} + 2^{80}$	95	4784	208

Table 4.1: Examples of families of genus 2 curves over $\mathbb{F}_{2^m}$ with appropriate parameters for comparison of security.

4.2.4 Mersenne prime family of curves

We now return to Example 4.2.3 and prove the existence of the family of curves of genus two over $\mathbb{F}_q$ whose group of $\mathbb{F}_q$-rational points of its Jacobian has size

divisible by a Mersenne prime ℓ. This family is such that there is a difference of a factor of m between the extension degrees of the minimal embedding field and the one suggested by the embedding degree k.

Proposition 4.2.7. *Let $q = 2^m$, and $p \geq 7$ be a prime. If $\ell = 2^p - 1$ is prime, then for each integer m such that $\lceil \frac{2p}{3} \rceil \leq m \leq p - 1$, there exists a genus two curve C over $\mathbb{F}_{2^m}$ with the property that $\#J_C(\mathbb{F}_{2^m}) = 2^{2m-p}\ell$, where $a_1 = -1$ and $a_2 = 2^m - 2^{2m-p}$. The embedding degree is $k = p$ and so the difference in size between the extension degrees of $\mathbb{F}_{q^k}$ and the minimal embedding field $\mathbb{F}_{2^p}$ is m.*

Proof. We first note that for $p \geq 7$, we have $m \geq 5$. Let us show that the conditions of Theorem 3.2.1 are met for the existence of genus two curves C when $a_1 = -1$ and $a_2 = 2^m - 2^{2m-p}$. Clearly a_1 is odd, and $|a_1| \leq 4\sqrt{q}$. Let us show $2\sqrt{q} - 2q \leq a_2 \leq 1/4 + 2q$, that is,

$$2^{m/2+1} - 2^{m+1} \leq 2^m - 2^{2m-p} \leq 1/4 + 2^{m+1}.$$

Clearly the second inequality holds. The first inequality holds if

$$2^{m/2+1} + 2^{2m-p} = 2^m(2^{1-m/2} + 2^{m-p}) \leq 2^m 3.$$

Since $0 < 2^{1-m/2} < 1$, then this holds if $m - p \leq 1$. Our restriction that $\lceil \frac{2p}{3} \rceil \leq m \leq p - 1$ implies $m - p \leq -1$, so we see this condition holds true.

Now let us show that $2^{\lceil m/2 \rceil}$ divides a_2.

$$2^{\lceil m/2 \rceil} \mid 2^m - 2^{2m-p} \iff 2m - p \geq \lceil m/2 \rceil$$

$$\iff \lfloor 3m/2 \rfloor \geq p$$
$$\iff m \geq \lceil \frac{2p}{3} \rceil.$$

Thus the condition holds.

Now let us show $\Delta = a_1^2 - 4a_2 + 8q$ is not a square in $\mathbb{Z}$. For contradiction, suppose $\Delta = 1 - 2^{m+2} + 2^{2m-p+2} + 2^{m+3} = 1 + 2^{2m-p+2} + 2^{m+2} = x^2$ for some integer x. Since Δ is odd, then x is odd, so let $x = 2c + 1$ for some integer c. Then Δ is a square if and only if $2^{2m-p}(2^{p-m} + 1) = c(c + 1)$. We apply Lemma 3.2.2, letting $a = 2m - p$ and $b = p - m$. We note that $a > 0$ since $m \geq \lceil \frac{2p}{3} \rceil$ implies $\lfloor \frac{3m}{2} \rfloor \geq p$, so $2m - p > 0$. Also $b > 0$ since $p - 1 \geq m$ implies $p - m > 0$. Thus Δ a square implies $2m - p \leq p - m$, that is, $m \leq \frac{2p}{3}$. Since p is prime, this is actually only if $m \leq \lfloor \frac{2p}{3} \rfloor < \lceil \frac{2p}{3} \rceil$. Therefore Δ is not a square in $\mathbb{Z}$ for $\lceil \frac{2p}{3} \rceil \leq m \leq p - 1$.

Now let us show $\delta = (a_2 + 2q)^2 - 4qa_1^2$ is not a square in $\mathbb{Z}_2$. That is, for $\delta = 2^x b$, we must show that either $b \not\equiv 1 \bmod 8$ or $x \equiv 1 \bmod 2$. Now

$$\begin{aligned}
\delta &= (2^m - 2^{2m-p} + 2^{m+1})^2 - 2^{m+2} \\
&= (2^m - 2^{2m-p})^2 + 2^{m+2}(2^m - 2^{2m-p}) + 2^{2m+2} - 2^{m+2} \\
&= 2^{2m+3} + 2^{2m} - 2^{3m-p+2} - 2^{3m-p+1} + 2^{4m-2p} - 2^{m+2} \\
&= 2^{m+2}(2^{m+1} + 2^{m-2} - 2^{2m-p} - 2^{2m-p-1} + 2^{3m-2p-2} - 1).
\end{aligned}$$

So we have that $b = 2^{m-2}(2^3 + 1) - 2^{2m-p-1}(2 + 1) + 2^{3m-2p-2} - 1$.

For $m \geq 5$, we have

$$\begin{aligned}
b &\equiv -2^{2m-p-1}3 + 2^{3m-2p-2} - 1 \bmod 8 \\
&\equiv 2^{3m-2p-2}(1 - 2^{p-m+1}3) - 1 \bmod 8.
\end{aligned}$$

Now, suppose $b \equiv 1 \bmod 8$. Then

$$b + 1 \equiv 2^{3m-2p-2}(1 - 2^{p-m+1}3) \equiv 2 \bmod 8.$$

By the same reasoning as in the proof of Proposition 3.2.3, $3m-2p-2$ cannot equal 0 or 2, and clearly cannot be greater than or equal to 3. If $3m-2p-2 = 1$, then $m = \frac{3+2p}{3}$. But p is prime and $p \neq 3$, so $m = \frac{3+2p}{3} \notin \mathbb{Z}$. This cannot happen as we require an integer m. Thus $b \not\equiv 1 \bmod 8$, and so δ is not a square in $\mathbb{Z}_2$. Therefore the conditions of Theorem 3.2.1 are satisfied for the existence of a genus two curve C over $\mathbb{F}_q$.

Now let us show that $\#J_C(\mathbb{F}_{2^m}) = 2^{2m-p}\ell$ whenever $a_1 = -1$ and $a_2 = 2^m - 2^{2m-p}$. We recall that $\#J_C(\mathbb{F}_q) = q^2 + a_1 a_2^a + a_1 + 1$. So

$$\begin{aligned} \#J_C(\mathbb{F}_{2^m}) = 2^{2m} - 2^{2m-p} &= 2^{2m-p}(2^p - 1) \\ &= 2^{2m-p}\ell. \end{aligned}$$

Now we find the embedding degree k with respect to $\ell = 2^p - 1$. We see that $\mathrm{ord}_\ell 2 = p$, so $\gcd(\mathrm{ord}_\ell 2, m) = 1$ since $m \leq p - 1$. Therefore by Lemma 3.1.2, $k = p$, and the difference in extension degrees between $\mathbb{F}_{q^k}$ and the minimal embedding field is $\frac{m}{\gcd(\mathrm{ord}_\ell 2, m)} = m$. Thus the proof of the proposition is complete. □

Chapter 5

Future Research and Conclusion

5.1 Constructing explicit curves

A systematic way of determining the explicit coefficients of a curve over $\mathbb{F}_q$ when given the (a_1, a_2) parameters that distinguish the $\mathbb{F}_q$-isogeny class of its Jacobian is not yet established. Complex multiplication (CM) methods, inspired by the CM algorithm proposed in [AM93], have been used for constructing elliptic curves in special cases [MNT01, CP01, BLS02, DEM05, BW05, Wen03]. The construction of hyperelliptic curves of genus two has begun to receive attention, as [Wen03] considered such curves over prime fields, [GHK$^+$05] gave a p-adic CM-method for ordinary curves over prime fields and [EL04] gave a Chinese remainder theorem (CRT) algorithm for ordinary curves of genus two.

These methods focus on supersingular and ordinary curves, and the published literature lacks a discussion of similar approaches for p-rank 1 curves (and occasionally excludes curves over binary fields). We imagine attention has been drawn to ordinary curves because of their nice canonical lift property, but we would like to explore such lifting methods for p-rank 1 curves. Then we hope to apply these methods to construct the family of 2-rank 1 curves

described in Chapter 3, so that one can construct such curves of cryptographic size.

Meanwhile, we have tried to determine restrictions on the coefficients of the curve that correspond to the power of two that divides $\#J_C(\mathbb{F}_q)$. This technique could aid in the construction of curves, as well as be insightful for point compression.

5.2 Point compression

In [Kin04], an algorithm for point compression is proposed when the order of an elliptic curve over $\mathbb{F}_{2^m}$ is divisible by a power of two. In our family of curves in Chapter 3, since $\#J_C(\mathbb{F}_{2^m})$ is divisible by a high power of two, these curves may lend themselves to point compression using similar methods.

5.3 Similar families for ordinary curves

We would like to examine ordinary curves using similar techniques that led to the family of 2-rank 1 curves described in Chapter 3. Following this, we would examine if there are curves in such a family that could be constructed using known CM-methods.

5.4 Conclusion

Hyperelliptic curves are receiving increased attention for use in discrete logarithm based cryptosystems. A primary focus involves the search for pairing-friendly curves, which have an embedding degree k small enough for computa-

tions to be feasible, but large enough for the discrete logarithm problem both on the curve and in the minimal embedding field to be intractable. We have constructed a sequence of $\mathbb{F}_q$-isogeny classes for a family of Jacobians of genus two, 2-rank 1 curves over $\mathbb{F}_q$, for $q = 2^m$, and their corresponding small embedding degrees. In particular, we gave examples of the parameters for such curves with embedding degree $k < (\log q)^2$, such as $k = 8, 13, 16, 23, 26, 37, 46, 52$, so that the computations in $\mathbb{F}_{q^k}$ may be feasible. Our family of curves also yields the ratio ρ often near 1 and never more than 2.

We have presented examples of elliptic curves and curves of genus two that demonstrate how the embedding degree k can fail to capture the security of a pairing-based cryptosystem. The difference in field sizes between $\mathbb{F}_{q^k}$ and the minimal embedding field can be seen any time $q = p^m$ for $m > 1$ and $\gcd(\mathrm{ord}_\ell p, m) \neq m$, and we emphasize that it is possible for the extension degrees to differ by a factor of m. It is of critical importance to check when working over fields of small characteristic. The possible substantial difference in the size of the fields has the implication in theory that there could be curves used in DL systems that are presently regarded as secure against pairing-based attacks but are in fact insecure.

Bibliography

[AM93] A. O. L. Atkin and F. Morain. Elliptic curves and primality proving. *Math. Comp.*, 61(203):29–68, 1993.

[BK98] R. Balasubramanian and N. Koblitz. The improbability that an elliptic curve has subexponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm. *J. of Cryptology*, 11(2):141–145, 1998.

[BLS02] P. S. L. M. Barreto, B. Lynn, and M. Scott. Constructing elliptic curves with prescribed embedding degrees. In *Security in Communication Networks - SCN 2002*, volume 2576 of *Lecture Notes in Comput. Sci.*, pages 257–267. Springer-Verlag, Berlin, 2002.

[Bir06] P. Birkner. Efficient divisor class halving on genus two curves. Cryptology ePrint Archive, Report 2006/257, 2006.

[BF01] D. Boneh and M. Franklin. Identity-based encryption from the Weil pairing. In *Advances in cryptology—CRYPTO 2001 (Santa Barbara)*, volume 2139 of *Lecture Notes in Comput. Sci.*, pages 213–229. Springer-Verlag, Berlin, 2001.

[BLS01] D. Boneh, B. Lynn, and H. Shacham. Short signatures from the Weil pairing. In *Advances in cryptology—ASIACRYPT 2001 (Gold Coast)*, volume 2248 of *Lecture Notes in Comput. Sci.*, pages 514–532. Springer-Verlag, Berlin, 2001.

[BLS04] D. Boneh, B. Lynn, and H. Shacham. Short signatures from the Weil pairing. *J. of Cryptology*, 17(4):297–319, 2004.

[BW05] F. Brezing and A. Weng. Elliptic curves suitable for pairing based cryptography. *Des. Codes Cryptogr.*, 37(1):133–141, 2005.

[Cal06] C. K. Caldwell. Heuristics: Deriving the Wagstaff Mersenne Conjecture. The prime pages: prime number research, records, and resources, 2006. Available at http://primes.utm.edu/mersenne/heuristic.html.

[CP01] C. Cocks and R. G. E. Pinch. Identity-based cryptosystems based on the Weil pairing. Unpublished manuscript, 2001.

[CF05] H. Cohen and G. Frey, editors. *Handbook of Elliptic and Hyperelliptic Curve Cryptography*. CRC Press, 2005.

[DH76] W. Diffie and M. E. Hellman. New directions in cryptography. *IEEE Trans. Information Theory*, IT-22(6):644–654, 1976.

[DEM05] R. Dupont, A. Enge, and F. Morain. Building curves with arbitrary small MOV degree over finite prime fields. *J. of Cryptology*, 18(2):79–89, 2005.

[EL04] K. Eisentraeger and K. Lauter. A CRT algorithm for constructing genus 2 curves over finite fields, 2004. To appear in Arithmetic, Geometry and Coding Theory - AGCT-10 (Marseille), 2005.

[FMR99] G. Frey, M. Müller, and H.-G. Rück. The Tate pairing and the discrete logarithm applied to elliptic curve cryptosystems. *IEEE Trans. Inform. Theory*, 45(5):1717–1719, 1999.

[FR94] G. Frey and H.-G. Rück. A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. *Math. Comp.*, 62(206):865–874, 1994.

[Gal01a] S. D. Galbraith. Supersingular curves in cryptography, full version. Available at http://www.isg.rhul.ac.uk/ sdg/ss.ps.gz.

[Gal01b] S. D. Galbraith. Supersingular curves in cryptography. In *Advances in Cryptology—ASIACRYPT 2001 (Gold Coast)*, volume 2248 of *Lecture Notes in Computer Science*, pages 495–513. Springer-Verlag, Berlin, 2001.

[GMV04] S. D. Galbraith, J. McKee, and P. Valença. Ordinary abelian varieties having small embedding degree. Cryptology ePrint Archive, Report 2004/365, 2004.

[GM05] S. D. Galbraith and A. J. Menezes. Algebraic curves and cryptography. *Finite Fields Appl.*, 11(3):544–577, 2005.

[GPS06] S.D. Galbraith, K.G. Paterson, and N.P. Smart. Pairings for cryptographers. Cryptology ePrint Archive, Report 2006/165, 2006. http://eprint.iacr.org/.

[GHK+05] P. Gaudry, T. Houtmann, D. Kohel, C. Ritzenthaler, and A. Weng. The p-adic CM-method for genus 2, 2005. Available at http://arxiv.org/abs/math.NT/0503148.

[JMS04] Michael Jacobson, Jr., Alfred Menezes, and Andreas Stein. Hyperelliptic curves and cryptography. In *High primes and misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams*, volume 41 of *Fields Inst. Commun.*, pages 255–282. Amer. Math. Soc., Providence, RI, 2004.

[Jou00] A. Joux. A one round protocol for tripartite Diffie-Hellman. In *The 4th International Symposium on Algorithmic Number Theory - ANTS-IV*, pages 385–394. Springer-Verlag, London, UK, 2000.

[Jou04] A. Joux. A one round protocol for tripartite Diffie-Hellman. *J. of Cryptology*, 17(4):263–276, 2004.

[Kin04] B. King. A point compression method for elliptic curves defined over GF(2^n). In *Public key cryptography—PKC 2004*, volume 2947 of *Lecture Notes in Computer Science*, pages 333–345. Springer-Verlag, Berlin, 2004.

[Kob87] N. Koblitz. Elliptic curve cryptosystems. *Math. Comp.*, 48(177):203–209, 1987.

[Kob89] N. Koblitz. Hyperelliptic cryptosystems. *J. of Cryptology*, 1(3):139–150, 1989.

[LS05] T. Lange and M. Stevens. Efficient doubling on genus two curves over binary fields. In *Selected areas in cryptography - SAC 2004*, volume 3357 of *Lecture Notes in Computer Science*, pages 170–181. Springer-Verlag, Berlin, 2005.

[MN02] D. Maisner and E. Nart. Abelian surfaces over finite fields as Jacobians. *Experiment. Math.*, 11(3):321–337, 2002. With an appendix by Everett W. Howe.

[MV05] G. McGuire and J. F. Voloch. Weights in codes and genus 2 curves. *Proc. Amer. Math. Soc.*, 133(8):2429–2437 (electronic), 2005.

[MOV93] A. J. Menezes, T. Okamoto, and S. A. Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field. *IEEE Transactions Information Theory*, 39(5):1639–1646, 1993.

[Mil86] V. S. Miller. Use of elliptic curves in cryptography. In *Advances in cryptology—CRYPTO '85 (Santa Barbara)*, volume 218 of *Lecture Notes in Comput. Sci.*, pages 417–426. Springer-Verlag, Berlin, 1986.

[MNT01] A. Miyaji, M. Nakabayashi, and S. Takano. New explicit conditions of elliptic curve traces for FR-reduction. *IEICE Transactions on Communications/Electronics/Information and Systems*, 2001.

[Age05] National Security Agency. The case for elliptic curve cryptography. National Security Agency Information Assurance for Industry report, 2005. Available at http://www.nsa.gov/ia/industry/crypto_elliptic_curve.cfm.

[Oor74] F. Oort. Subvarieties of moduli spaces. *Invent. Math.*, 24:95–119, 1974.

[PH78] S. C. Pohlig and M. E. Hellman. An improved algorithm for computing logarithms over GF(p) and its cryptographic significance. *IEEE Transactions on Information Theory*, 24:106–110, 1978.

[RS02] K. Rubin and A. Silverberg. Supersingular abelian varieties in cryptology. In *Advances in cryptology—CRYPTO 2002*, volume 2442 of *Lecture Notes in Computer Science*, pages 336–353. Springer-Verlag, Berlin, 2002.

[Rüc90] H.-G. Rück. Abelian surfaces and Jacobian varieties over finite fields. *Compositio Math.*, 76(3):351–366, 1990.

[SOK00] R. Sakai, K. Ohgishi, and M. Kasahara. Cryptosystems based on pairing. In *Symposium on Cryptography and Information Security - SCIS 2000*, 2000.

[Sil03] A. Silverberg. Supersingular abelian varieties and their applications to cryptography. Lecture given in Number Theory Seminar at University of Texas, October 2003.

[Tat66] J. Tate. Endomorphisms of abelian varieties over finite fields. *Invent. Math.*, 2:134–144, 1966.

[WM71] W. C. Waterhouse and J. S. Milne. Abelian varieties over finite fields. In *1969 Number Theory Institute (Proceedings of Symposia in Pure Math., Vol. XX)*, pages 53–64. Amer. Math. Soc., Providence, R.I., 1971.

[Wen03] A. Weng. Constructing hyperelliptic curves of genus 2 suitable for cryptography. *Math. Comp.*, 72(241):435–458, 2003.

Vita

Laura Michelle Hitt was born in Webster, Texas on March 8, 1979, the daughter of Ricky and Linda Hitt. In 1997, she graduated from Clear Creek High School in League City, TX, just outside of Houston, TX. She then attended Samford University in Birmingham, Alabama, where she graduated with a Bachelor of Science in Mathematics in May of 2001. In September of 2001, she began work on her Doctorate of Philosophy in Mathematics at the University of Texas at Austin. At UT-Austin, Laura has held positions as teaching assistant, research assistant and instructor.

Permanent address: 6809 Shoal Creek Blvd., Austin, Texas 78757

This dissertation was typeset with LaTeX[‡] by the author.

[‡]LaTeX is a document preparation system developed by Leslie Lamport as a special version of Donald Knuth's TeX Program.